Santa Clara High Technology Law Journal

Volume 17 | Issue 2 Article 1

January 2001

Should Junk E-Mail be Legally Protected?

Joseph D'Ambrosio

ARTICLES

Should "Junk" E-Mail Be Legally Protected?

Joseph D'Ambrosio[†]

TABLE OF CONTENTS

[†] The author is an associate with the firm of Ford Marrin Esposito Witmeyer & Gleser, L.L.P. in New York City. He specializes in general commercial litigation, including e-commerce and Internet-related litigation. He is a graduate *cum laude* of the George Washington University Law School where he served as Notes Editor of the Journal of International Law & Economics.

I. INTRODUCTION

As both the Internet[1] and the volume of its users continue to grow,[2] it is not surprising that legal problems associated with the Internet also continue to develop in every area of the law. This article explores a narrow issue that has serious First Amendment implications: whether 'junk' e-mail (also called 'bulk' e-mail or 'spam') should be legally protected. First, this article defines junk e-mail and attempts to explain why on-line computer services are trying desperately to curtail it. Second, this article reviews recent cases that have dealt specifically with junk e-mail in the First Amendment context. Third, this article assesses whether junk e-mail may be afforded protection under state common or federal statutory law.

II. WHAT IS JUNK E-MAIL?

As e-mail[3] becomes a popular alternative to traditional letter writing, advertising companies, who ordinarily send bulk mail such as catalogs, brochures, pamphlets and other forms of direct mail, are frequently attempting to tap into this potentially massive audience by sending unsolicited e-mail messages to hundreds of thousands of e-mail users worldwide. From an advertising standpoint, one of the more important benefits of e-mail advertising compared to traditional forms (which advertising companies were quick to recognize) is that it is virtually cost-free to the advertiser. Other than a basic service fee paid to companies who distribute the e-mail ads, there is no per-message charge. Additionally, advertising by e-mail is much faster than traditional direct mail because the messages reach their destinations within minutes. This type of direct on-line advertising is known by various terms, including bulk e-mail, junk e-mail and spam.[4]

---

[1] The Internet has been defined as "a decentralized, global communications medium that links people, institutions, corporations and governments around the world." Cyberspace Communications, Inc. v. Engler, 55 F. Supp. 2d 737, 741 (E.D. Mich. 1999) (citing ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996)).

[2] Recent estimates suggest that the Internet connects more than 159 countries and over 100 million users. *See* ACLU v. Johnson, 4 F. Supp. 2d 1029, 1031 (D.N.M. 1998).

[3] Almost all Internet users are able to procure an e-mail address that allows them to communicate with other users. *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 165 (S.D.N.Y. 1997).

[4] One court has defined spam as "unsolicited commercial bulk e-mail akin to 'junk mail' sent through the postal mail." Am. Online v. LCGM, Inc., 46 F. Supp. 2d 444, 446 n.1 (E.D. Va. 1998).

Recognizing the potential market for direct e-mail advertising services, many companies now are founded for the sole purpose of distributing the advertisements of various other commercial entities. In fact, companies now sell software designed specifically to facilitate sending junk e-mail.[5] However, due to the vast amount of unsolicited e-mail ads filling up Internet users' mailboxes, most e-mail users have not been thrilled with this new development.

Many Internet e-mail customers now complain to their respective Internet Service Providers (ISPs), such as America Online, CompuServe and Prodigy. As a result, ISPs are forced to respond or risk losing their subscribers. The usual, first response of ISPs is to notify these junk advertisers that they are prohibited from using their respective computer networks to send unsolicited e-mail. Predictably, the advertisers rarely stop sending the e-mail. Because these notices usually do not solve the problem, ISPs create software programs to prevent dissemination of this junk e-mail.[6] Undeterred, the advertising companies seem to find ways to protect their messages from the software by concealing their names and addresses. The inability of ISPs to compromise with junk advertisers has spawned multiple lawsuits, seeking both equitable remedies, to prevent advertisers from sending junk email, and legal relief in the form of monetary damages.

Because of a lack of immediate remedies, Internet users themselves have begun to step up efforts to eliminate spamming because it both interferes with their use of e-mail and violates the rules of 'netiquette' (rules of etiquette in cyberspace). One web site conducting a survey on opinions of junk e-mail reveals what one might expect: the vast majority of people oppose spamming.[7] Not surprisingly, a search of the Internet reveals numerous sites lobbying for a ban on junk e-mail[8] and other sites offering to help users stop unwanted junk e-mail.[9] Despite such sites, however, the problem of junk e-mail has yet to be fully resolved.

---

[5] *See, e.g.*, INTERMEDIA COMMUNICATIONS *at* http://www.intermedia.com; ROD'S NETWORKING SERVICES *at* http//www.the-peoples.net (last visited on Apr. 11, 2001).

[6] *See, e.g.*, THE SPAM FILTER *at* http://www.scot.demon.co.uk/spam-filter.html (last visited on Apr. 11, 2001); SUPER MAIL *at* http://www.supermail.com (last visited Apr. 11, 2001); CATALOG.COM *at* http://www.catalog.com (last visited Apr. 11, 2001).

[7] *See* Survey.com, *1997 Junk E-mail Survey Results at* http://www.survey.com/junkresults.html (last visited Apr. 11, 2001).

[8] *Id.*

[9] *See e.g.*, NOJUNK.HTML *at* http://www.glr.com/nojunk.html (last visited Apr. 11, 2001). If you feel a need to voice your opinion on this issue, please contact your local Congressperson or Internet service provider and let them know how you feel about spam.

III. IS JUNK E-MAIL PROTECTED SPEECH?

The First Amendment to the United States Constitution states "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press."[10] Junk advertisers often cite the First Amendment as protecting the transmission of junk e-mail. However, because the First Amendment applies only to laws enacted by Congress, junk advertisers must first prove that an ISP's blocking of junk e-mail somehow arises from government or state action and therefore abridges the advertisers' First Amendment rights.[11]

In *Cyber Promotions, Inc. v. America Online, Inc.*, (*Cyber Promotions I*),[12] Cyber Promotions, a private on-line advertising company, brought claims under state law and the Computer Fraud and Abuse Act[13] against America Online (AOL). The suit alleged that AOL sent e-mail bombs[14] to Cyber's service providers in response to Cyber Promotions sending millions of junk e-mails to AOL customers.[15] This bombing allegedly resulted in the cancellation of various contracts between Cyber and its service providers. Cyber further alleged that AOL's private action constituted state action because of the close nexus between AOL's action and the government.[16]

The court rejected this argument because it failed to satisfy the three tests outlined by the Supreme Court to determine when private action may be considered government or state action.[17] First, under the *exclusive public functions test*, the court considers whether the private entity (AOL) is exercising powers that are the exclusive

---

[10] U.S. CONST. amend. I.

[11] *See* Hurley v. Irish-Am. Gay Group of Boston, 515 U.S. 557 (1995); *see also* Hudgens v. Nat'l Labor Relations Bd. (NLRB), 424 U.S. 507 (1976).

[12] Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436 (E.D. Pa. 1996) [hereinafter *Cyber Promotions I*].

[13] 18 U.S.C. § 1030(a)(5)(A) (1994) (stating that "whoever knowingly causes the transmission of a program, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished.").

[14] An 'e-mail bomb' is one where the sender executes an automated script with a chain of source routed messages that are delivered to a single server that usually results in the server being shut down from the e-mail overload. *See* Tim Bass et al., *E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand Measures*, IEEE NETWORKS Vol. 12 No. 2, 10, Mar.-Apr. 1998, *available at* http://silkroad.com/papers/html/bomb (last visited on Apr. 11, 2001).

[15] *Cyber Promotions I*, 948 F. Supp. at 437.

[16] *Cf.* Blum v. Yaretsky, 457 U.S. 991, 1004 (1982).

[17] *Cyber Promotions I*, 948 F. Supp. at 441.

prerogative of the government.[18] Since the Internet is owned by private entities, it fails the exclusive public functions test.

Second, under the *acting in concert test*, the court considers whether "'the private entity has acted with the help of or in concert with state officials.'"[19] Cyber argued that AOL was acting with the help of the court (indicating government action) by seeking injunctive relief in its counterclaim. The court quickly rejected this argument based upon long-standing precedent that holds filing a lawsuit alone does not transform private action into government action under color of law. Thus, Cyber failed to satisfy the acting in concert test.

Finally, under the *joint participant test*, the court considers whether the private entity and the government are in a position of interdependence.[20] Again, the court held that the doctrine did not apply to the facts of *Cyber Promotions I*. As a result, the court found that the First Amendment was not implicated.

IV. CAN THE COMMON LAW PROTECT AGAINST SPAMMING?

ISPs have also looked to state common law to protect their rights against spammers.[21] One such case is *CompuServe Inc. v. Cyber Promotions, Inc.* (*Cyber Promotions II*), another case involving Cyber Promotions.[22] In this case, CompuServe sued Cyber Promotions for trespass to personal property. Cyber again relied upon the First Amendment as its affirmative defense. In granting CompuServe's motion for a preliminary injunction (which prevented Cyber from sending junk e-mail during the pendency of the case), the court also held that CompuServe stated a viable claim for trespass under Ohio state law.[23] The court relied upon Section 217(b) of the Restatement (Second) of Torts to affirm CompuServe's trespass claim. Section

---

[18] *See* Island Online, Inc. v. Network Solutions, Inc., 119 F. Supp. 2d 289 (E.D.N.Y. 2000). Island Online sued Network Solutions, Inc., a major domain name registrar, alleging violations of free speech and due process after Network Solutions refused to register names that included obscene words. The court granted Network Solutions's motion for summary judgment on the grounds that registering domain names is a private, rather than a public, function. *Id.*

[19] *Cyber Promotions I*, 948 F. Supp. at 441 (citing McKeesport Hosp. v. Accreditation Council for Graduate Med. Educ., 24 F.3d 519, 524 (3d Cir. 1994)).

[20] *Cyber Promotions I*, 948 F. Supp. at 441. *See also* Mark v. Borough of Hatboro, 51 F.3d 1137, 1142 (3d Cir. 1995) (quoting Krynicky v. Univ. of Pittsburgh, 742 F.2d 94, 98 (3d Cir. 1984)).

[21] *See generally* Mark D. Robins, *Electronic Trespass: An Old Theory in a New Context*, 15 COMPUTER LAW 1 (1998).

[22] CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) [hereinafter *Cyber Promotions II*].

[23] *Id.* at 1017.

217(b) states that a trespass may be committed by intentionally using or intermeddling with another person's chattels (personal property).[24] Intermeddling is defined as "intentionally bringing about a physical contact with the chattel."[25] The court then relied upon cases from other jurisdictions to support the proposition that "electronic signals generated and sent by computer" are "sufficiently physically tangible to support a trespass cause of action."[26] The court found that CompuServe alleged sufficient harm to its chattels to state a trespass cause of action under Section 217 of the Restatement.

In identifying the harm to CompuServe from Cyber's actions, the court observed, "many subscribers have terminated their accounts specifically because of the unwanted receipt of bulk e-mail messages."[27] In addition, the court noted that comment 'e' to Section 218 of the Restatement gives the property owner a "privilege to use reasonable force to protect his possession."[28] In *Cyber Promotions II*, Cyber's efforts to circumvent CompuServe's security measures by concealing the true domain name and origin of the messages prevented CompuServe from exercising this privilege.[29]

Cyber unsuccessfully argued, as it did unsuccessfully in *Cyber Promotions I*, that its actions were protected under the First Amendment. In particular, Cyber argued that CompuServe assumed the role of postmaster (for e-mail purposes) and should therefore be subject to the strictures of the First Amendment—like a government-run post office.[30] Nevertheless, the court relied upon the decision in *Cyber Promotions I* in finding that CompuServe was *not* a state actor. More importantly, the court noted that there were still alternative means of advertising; through traditional channels such as direct United States mail and over the Internet through designated commercial sites.

In *America Online, Inc. v. IMS*, AOL relied upon the same common law trespass argument utilized in *Cyber Promotions II* against another junk advertiser.[31] Indeed, the court noted "the *CompuServe* case is so strikingly similar to the current litigation and

---

[24] *Id.* at 1017.

[25] *Id.*

[26] *Id.*

[27] *Id.* at 1023.

[28] *Cyber Promotions II*, 962 F. Supp. at 1023.

[29] Please check the links, *supra* note 6, for detailed information on the service providers' efforts to eliminate junk e-mail.

[30] *Cyber Promotions II*, 962 F. Supp. at 1026.

[31] Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) [hereinafter *Am. Online I*].

the trespass law of Virginia is so close to that of Ohio, [therefore] we will rely on the reasoning of *Cyber Promotions [II]*."[32] Since each of the common law elements[33] of trespass were met, the court granted AOL's motion for summary judgment.[34] Based on these cases, the common law doctrine of trespass to chattels appears to be a potent weapon for Internet service providers in their fight against spam.

V. CAN FEDERAL TRADEMARK LAW PROTECT AGAINST SPAMMING?

Recently, AOL has relied upon the Lanham Trademark Act[35] in its fight against spammers.[36] In *America Online, Inc. v. LCGM, Inc.*, AOL alleged that the defendant spammers transmitted ninety-two million unsolicited messages to AOL customers within a seven month period.[37] AOL sued for various claims of relief, including two claims under the Lanham Act. First, AOL brought a false designation claim against LCGM, arguing that LCGM falsely designated the origin of the junk e-mails by incorporating the <aol.com> designation in its e-mail headers.[38] The court agreed with AOL, holding that the LCGM's use of the <aol.com> designation in their headers would likely cause AOL's customers to believe that AOL authorized these unsolicited e-mails when it did not.

Second, AOL claimed that LCGM's actions diluted the <aol.com> service mark in violation of the Lanham Act.[39] As a preliminary matter, the court found that AOL's service mark was *distinctive* because it was well-recognized throughout the world.[40]

---

[32] *Id.*

[33] Vines v. Branch, 418 S.E.2d 890, 894 (Va. 1992) (finding that Virginia courts had recognized a common law tort for trespass to chattels. "Where a person has illegally seized the personal property of another and converted it to his own use, the owner may bring an action in trespass.. . .."). The court relied on the Restatement (Second) of Torts § 217(b) to determine the elements of the cause of action. *Id.*

[34] *Am. Online I*, 24 F. Supp 2d. at 550 (holding, as a matter of law, the defendant had intentionally contacted AOL's computer network without AOL's authorization causing damage to AOL's personal property).

[35] 15 U.S.C.A. § 1051-1125 (2001).

[36] *See* Bruce Balestier, *Queens Company Hit with Big Fine for E-Mail 'Spam,'* N.Y.L.J., Dec. 14, 1999, at 1 (reporting that a federal magistrate judge granted AOL a default judgment and permanent injunction against a spammer who transmitted millions of unsolicited e-mails touting apricot seeds as a cancer cure).

[37] Am. Online, Inc. v LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Ca. 1998) [hereinafter *LCGM*].

[38] *See* 15 U.S.C.A. § 1125(a)(1) (2001).

[39] *See* 15 U.S.C.A. § 1125(c)(1) (2001).

[40] *LCGM*, 46 F. Supp. 2d at 450. A trademark must be at least "distinctive" in order to prevail on a dilution claim. *See* Hormel Foods Corp. v. Jim Henson Prods., Inc., 73 F.3d 497, 506 (2nd

The court then held that the AOL mark had been diluted by association with LCGM's bulk e-mails.

Based upon the decision in *LCGM*, it appears that ISPs have found another weapon in their fight against spam.[41] Further, this is a potentially powerful weapon because it will be much more difficult for spammers to raise the First Amendment as a defense to trademark infringement and dilution claims. It remains to be seen, however, whether federal trademark laws will be readily available in every situation in which junk e-mail is transmitted. For instance, if the defendants in *LCGM* had transmitted their bulk e-mails *without* the <aol.com> designation in the origination header, it is unlikely that AOL could have brought the Lanham Act claims. As a result, the common law trespass claims discussed above may be the ISPs' most consistent and effective tool in their fight against spam.[42]

VI. WHO ARE THE SPAMMERS?

Today, many companies seeking to advertise their products or services via e-mail engage the services of independent e-mailers, or contract e-mailers. These contract e-mailers typically charge a fee based on the number of e-mails transmitted or the number of responses to such e-mails received by the customer company. Thus, another remedy for ISPs is to hold the customer company liable for actions of its agent e-mail contractor. For an ISP to hold the customer company liable for the unsolicited bulk e-mails sent by contract e-mailers, however, the ISP must show that contract e-mailers actions were subject to the customer company's control.

In *America Online, Inc. v. National Health Care Discount, Inc.*,[43] this agency issue was addressed for the first time in the context of a junk e-mail case. AOL brought suit against National Health Care Discount (NHCD) for the transmission of millions of unsolicited e-mails relating to NHCD's optical and dental service plans.[44] The

---

Cir. 1996).

[41] Other recent cases in which on-line service providers have successfully asserted trademark claims against bulk e-mailers are Am. Online v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998) and Hotmail Corp. v. Van$ Money Pie, Inc., 47 U.S.P.Q. 1020 (N.D. Cal. 1998).

[42] Evidence of the continued importance of state common law in the fight against junk e-mail is the fact that America Online asserted the same trespass theory in both *LCGM* and *IMS* that was successfully employed in the *CompuServe* case. *See supra* notes 12, 22, 31.

[43] Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 121 F. Supp. 2d 1255 (N.D. IA 2000) [hereinafter *NHCD*].

[44] *Id.* at 1262 (accounting for NHCD's entry into agreements with dentists and eye care professionals to offer discounted services to the general public where members would pay a fee to NCHD for access to these discounted services).

record showed that over seventy-six million e-mails relating to NHCD had been transmitted on AOL's network.[45] The record also revealed that NHCD was contacted by several contract e-mailers who agreed to advertise on behalf of NCHD for a fee.[46]

AOL alleged violations of the Computer Fraud and Abuse Act, the Virginia Computer Crimes Act and common law trespass to chattels. In response to AOL's motion for summary judgment, the court concluded that AOL would be entitled to summary judgment only if AOL could prove that the contract e-mailer was an agent of NHCD, thereby making NHCD liable for the acts of the contract e-mailer.[47] Further, whether the contract e-mailers were agents of NHCD was a genuine issue of material fact that precluded the court from granting AOL's motion for summary judgment.[48] Although NHCD asserted constitutional defenses in its answer, the court did not address these issues in its opinion.[49] Instead, the constitutional defenses were preserved for trial.[50]

NHCD appears to create a potential shield from liability for companies seeking to advertise their products and services over the Internet. If companies continue to employ contract e-mailers to perform their on-line advertising, ISPs such as AOL may find it more difficult to hold the companies directly liable.[51] Of course, it will be interesting to see whether other courts apply the reasoning in *NHCD*. ISPs may need to decide whether it is strategically viable to attempt to hold the companies directly liable or whether it makes more sense simply to stop the contract e-mailers from sending the unsolicited e-mail.

---

[45] *Id.*

[46] *Id.* at 1262-63 (describing that NHCD agreed to pay the contract e-mailer $1.00 for each 'lead' obtained via e-mail advertising). A 'lead' is a response to an e-mail. *Id.*

[47] *Id.* at 1267-71. Virginia agency law would govern because the court concluded that Iowa (forum) choice of law principles favored application of Virginia substantive law. According to the court, Virginia is the most interested state because it is AOL's home state and AOL's servers are located there. *Id.*

[48] *Id.* at 1280.

[49] *NHCD*, 121 F. Supp. 2d at 1280.

[50] *Id.*

[51] In the normal case, on-line service providers likely will develop enough facts to prove an agency relationship. Although on-line service providers have the ability to shut down the contract e-mailers, their real goal is to deter the individuals who employ these contract e-mailers. One way to deter these companies is to hold them liable for the actions of contract e-mailers. *NHCD*, however, appears to make that more difficult.

VII. WILL FEDERAL LEGISLATION BE PASSED TO REGULATE SPAMMING DIRECTLY?

On March 25, 1999, Senator Frank H. Murkowski (R-Alaska) introduced Senate Bill 759,[52] the *Inbox Privacy Act of 1999* (1999 Act)[53] that would specifically regulate the transmission of unsolicited e-mail on the Internet.[54] If passed by Congress, the 1999 Act would expressly preempt *state* law, which likely includes state common law remedies for trespass discussed above.[55] The 1999 Act would also give ISPs and their customers the option of whether they wished to receive unsolicited e-mail. In particular, section two states that "[a] person may not initiate the transmission of unsolicited commercial electronic mail[56] to another person if such other person submits to the person a request that the initiation of the transmission of such mail by the person to such other person not occur."[57]

The 1999 Act allows ISPs or interactive computer service providers[58] to bring a civil action for damages within one year of discovery of the violation.[59] Damages in this situation are capped at $50,000 for each day that the violation continues.[60]

The 1999 Act also authorizes the Federal Trade Commission (FTC) to "prescribe rules for defining and prohibiting deceptive acts or practices in connection with . . . the sale or services on or by means of the Internet."[61] Additionally, the 1999 Act gives the FTC power to investigate alleged violations.[62] Nevertheless, there has been no activity on this bill for the past year. As a result, it is difficult to tell whether the bill will ever be passed.

---

[52] Inbox Privacy Act of 1999, S. 759, 106th Cong. (1999).

[53] *Id.* (stating that the purpose of the law is "[t]o regulate the transmission of unsolicited commercial e-mail on the Internet, and for other purposes.").

[54] This bill was co-sponsored by Senators Robert G. Torricelli (D-N.J.), Conrad R. Burns (R-Mont.), Harry Reid (D-Nev.), Richard J. Durbin (D-Ill.) and Olympia J. Snowe (R-Me).

[55] *See id.* § 7 ("This Act preempts any State or local laws regarding transmission or receipt of commercial electronic e-mail.").

[56] *Id.* § 8(1). ("[Commercial Electronic Mail] means any electronic mail or similar message whose primary purpose is to initiate a commercial transaction, not including messages sent by persons to others with whom they have a prior business relationship.").

[57] *Id.* § 2(a)(2) (stating that the request "may take any form appropriate to notify a person who initiates the transmission . . . of the request.").

[58] *Id.* § 8(3). ("[Interactive Computer Service Provider means] a provider of an interactive computer service (as that term is defined in § 230(e)(2) of the Communications Act of 1934 (47 U.S.C. § 230(e)(2)).").

[59] Inbox Privacy Act of 1999, S. 759, 106th Cong. § 6(b)(1) (1999).

[60] *Id.* § 6(b)(2)(A).

[61] *Id.* § 3(a)(1).

[62] *Id.* § 4(a)(1).

More recently in the House of Representatives, Representatives Heather Wilson (R-N.M.) and Gene Green (D-Tex.) introduced House Bill 3113, the *Unsolicited Commercial Electronic Mail Act of 2000* (2000 Act).[63] The 2000 Act was designed "to protect individuals, families and Internet service providers from unsolicited and unwanted electronic mail."[64] On July 18, 2000, the bill passed by a vote of 427 to 1 in the House and is currently being considered by the Senate.

The 2000 Act would impose a criminal penalty for sending "unsolicited commercial electronic mail containing *fraudulent* routing information."[65] It also would require the sender of *any* unsolicited commercial e-mail to include a valid return address to which the recipient may send a reply indicating a desire not to receive *any* additional e-mail.[66] Further, the 2000 Act would require the sender to provide a means by which the recipient may elect not to receive any further e-mail from the sender.[67] Not only would the 2000 Act protect individuals, it also would give ISPs broad discretion to block what they consider to be unlawful transmissions by immunizing them from liability.[68]

With respect to administering the 2000 Act, the FTC is given broad authority to regulate compliance.[69] If the FTC believes that

---

[63] Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. (2000). Interestingly, like the proposed Senate legislation, *supra* note 52, the Unsolicited Commercial Electronic Mail Act of 2000 has received bipartisan support. On May 24, 1999, Rep. Green had introduced a similar bill, House Bill 1910, popularly called the "E-Mail User Protection Act." E-Mail User Protection Act, H.R. 1910, 106th Cong. (1999). House Bill 1910 would prohibit the sending of unsolicited bulk e-mail containing false sender information, a false return address or other false and misleading information contained in the header of the e-mail designed to conceal the sender's identity. Like the proposed Inbox Privacy Act of 1999, the E-Mail User Protection Act would also prohibit the transmission of unsolicited mail if a recipient opts out of future mailings. Further, House Bill 1910 makes it illegal to sell or distribute computer software designed to evade the provisions of the bill.

[64] Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. (2000).

[65] *Id.* § 4 (emphasis added). This section also would amend 18 U.S.C. § 1030 by making it unlawful to intentionally initiate:

> the transmission of any unsolicited commercial electronic mail message to a protected computer in the United States with knowledge that any domain name, header information, date or time stamp, originating electronic mail address, or other information identifying the initiator of the routing of such message, that is contained in or accompanies such message, is false or inaccurate.

Id. § 4(d).

[66] *Id.* § 5(a)(1).

[67] *Id.* § 5(a)(3)(B).

[68] *Id.* § 5(c)(1) (providing that ISPs cannot be held liable for damages so long as they act with good faith belief that the blocked transmissions violate the 2000 Act).

[69] *Id.* § 6.

violations have occurred, it must notify the alleged violators and demand that they cease and desist from committing any further violations.[70] If the notice does not deter the violators, the FTC has the authority to file a complaint against the alleged violators.[71]

More importantly, and for the purposes of this article, Section 6 of the 2000 Act expressly permits private causes of action[72] for both injunctive[73] and monetary[74] relief. The monetary relief recoverable is either the actual monetary loss or $500 for each violation, not to exceed $50,000.[75] In the case of a willful violation, the court may award damages three times the amount authorized under subsection (1).[76] Additionally, the 2000 Act allows a prevailing party to recover costs and attorneys fees.[77] This provision will likely promote the filing of lawsuits.

Finally, state law addressing unsolicited e-mail is partially preempted to the extent that the state law is inconsistent with the 2000 Act.[78] The preemption is incomplete, however, because the 2000 Act expressly states that it "shall not preempt any civil remedy under State trespass or contract law . . . arising from the unauthorized transmission of unsolicited commercial electronic mail messages."[79]

No doubt recognizing the First Amendment concerns of regulating commercial speech of this type, the House set forth its

---

[70] Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 6(a)(1)-(2) (2000).

[71] *Id.* § 6(4)(A) (requiring the alleged violator to respond to the allegations in the complaint within fifteen days).

[72] *Id.* § 6(b)(1).

[73] *Id.* § 6(b)(1)(A).

[74] *Id.* § 6(b)(1)(B).

[75] *Id.* § 6(b)(1)(B)(i)-(ii).

[76] Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 6(2) (2000).

[77] *Id.* § 6(3).

[78] Not surprisingly, Microsoft's home state, Washington, was one of the first states to pass anti-spam legislation. WASH. REV. CODE ANN. § 19.190.010 (West 2000). Other states have also passed legislation directly regulating the transmission of unsolicited e-mail. VA. CODE ANN. § 18.2-152.4(A)(7) (Michie 2000) (making it unlawful to "falsify or forge electronic e-mail transmission information in connection with the transmission of unsolicited bulk electronic mail"); ILL. ANN STAT. ch. 815, para. 511/10 (2000) (making it unlawful to "initiate an unsolicited electronic mail advertisement . . . if it contains false or misleading information in the subject line"); CAL. BUS. & PROF. CODE § 17538.4 (West 2000) ("no person . . . shall electronically mail . . . unsolicited advertising material unless . . . that person establishes a . . . valid sender operated return e-mail address . . . that the recipient . . . may . . . e-mail to notify the sender not to e-mail any further unsolicited documents.").

[79] Unsolicited Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 6(b) (2000). The fact that state trespass law is expressly mentioned supports the belief that Congress was aware of the recent court decisions discussed, *supra* notes 22 and 31.

findings and policy in Section (2)(a) of the 2000 Act. As a preliminary matter, the House explicitly states that the "[t]here is a right of free speech on the Internet."[80] Additionally, the House notes that "[t]he Internet has increasingly become a critical mode of global communication and now presents unprecedented opportunities for the development and growth of global commerce and an integrated world economy."[81] The House also observed that "[u]nsolicited commercial electronic mail can be an important mechanism through which businesses advertise and attract customers in the on[-]line environment."[82]

On the other hand, the House also expressed the majority view that junk e-mail imposes significant costs on individual recipients "for the storage of such mail, or for time spent accessing, reviewing, and discarding such mail, or for both."[83] Moreover, the House found that junk e-mail "imposes significant monetary costs on Internet access services . . . negatively affecting the quality of service provided to customers of Internet access service."[84] Most importantly, Congress acknowledged that junk e-mail "may invade the privacy of recipients."[85]

The purpose of the Congressional findings is to demonstrate that the law is *rationally related* to an *important government interest.* These findings also reflect an attempt by Congress to balance the free speech rights of senders of unsolicited commercial e-mail against the hardship such e-mails pose to individuals and ISPs. If the 2000 Act is passed and subsequently challenged on First Amendment grounds, as this article suggests, courts will likely look to the law's legislative findings in evaluating its constitutionality. The question remains whether the identified burdens on recipients and ISPs justify the restrictions imposed on the commercial e-mailers. Since the burden on recipients is largely limited to clicking 'delete,' the real burden is the potential overload of system networks resulting in less efficient access for customers.

---

[80] *Id.* § 2(a)(1).
[81] *Id.* § 2(a)(2).
[82] *Id.* § 2(a)(3).
[83] *Id.* § 2(a)(4).
[84] *Id.* § 2(a)(5).
[85] Uniform Commercial Electronic Mail Act of 2000, H.R. 3113, 106th Cong. § 2(a)(9) (2000).

VIII. WILL THE PROPOSED FEDERAL LAWS WITHSTAND FIRST AMENDMENT SCRUTINY?

If Congress passes one of the bills discussed above, the difficulty of proving state action will be largely eliminated.[86] The stage then would be set for a serious First Amendment challenge to the restrictions imposed on spammers. The Supreme Court has explicitly held that commercial speech is afforded First Amendment protection as was the case in *Virginia State Bd. of Pharm. v. Virginia Citizens Consumer Council, Inc.*, where the fact that the speaker's motivation was an economic one "hardly disqualifie[d] him from protection under the First Amendment."[87] Further, the Court stated, "[i]t is clear . . . that speech does not lose its First Amendment protection because money is spent to project it, as in a paid advertisement of one form or another."[88]

The Court has never held, however, that commercial speech is entitled to the same protections as other forms of speech.[89] In *Central Hudson Gas v. Public Service Comm.*, the Court established a four-prong test for evaluating commercial speech restrictions (the *Central Hudson Test*).[90] The first prong is whether the speech at issue concerns lawful activity and is not misleading; unlawful and misleading content is not protected under the First Amendment.[91] Because the proposed federal legislation regulates *all* unsolicited commercial e-mail, it will likely capture at least *some* lawful and non-misleading activity.[92] The second prong is whether the asserted governmental interest in regulating the speech is substantial.[93] Given the Court's deference to the legislature, this article assumes that the Court will find the government's interest in regulating unsolicited

---

[86] The prohibitions of the First Amendment extend to states and their political subdivisions through the Fourteenth Amendment's due process and equal protection clauses. *See* Gitlow v. New York, 268 U.S. 652 (1925); Lovell v. City of Griffin, 303 U.S. 444 (1938).

[87] Virginia State Bd. of Pharm. v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 761 (1976).

[88] *Id.* at 761-62 (1976). Presumably, the language "one form or another" would extend to e-mail.

[89] Ohralik v. Ohio State Bar Ass'n., 436 U.S. 447, 456 (1978) ("We have not discarded the 'common sense' distinction between speech proposing a commercial transaction . . . and other varieties of speech.").

[90] Central Hudson Gas v. Public Service Comm., 447 U.S. 557 (1980).

[91] *Id.* at 566.

[92] Although some junk e-mail probably involves unlawful activity and may be deemed misleading, this article presumes that a spammer challenging the legislation will be able to satisfy the first part of the *Central Hudson Test.*

[93] For this part, the findings and policy of the legislation discussed above will be critical.

commercial e-mail to be substantial.

The third and fourth prongs of the test are more problematic for the proposed legislation to satisfy.[94] The third prong asks whether the regulation directly advances the government interests asserted.[95] The fourth prong asks whether the regulation is not more extensive than is necessary to serve that interest.[96] In other words, used together, "[t]he last two steps of the *Central Hudson* analysis basically involve a consideration of the 'fit' between the legislature's ends and the means chosen to accomplish those ends."[97] Further, the government's burden "is not satisfied by mere speculation or conjecture; rather a governmental body seeking to sustain a restriction on commercial speech must demonstrate that the harm it recites are real and that its restriction will in fact alleviate them to a material degree."[98]

Applying the last two *Central Hudson* prongs to the proposed federal legislation, it is not clear whether the legislation will withstand constitutional scrutiny. Arguably, the third prong will be satisfied because the government's interest in protecting recipients right to privacy is protected by giving them the option to elect not to receive future e-mails from the sender. Additionally, assuming that many recipients elect not to receive future e-mails from senders, the volume of unsolicited commercial e-mails will be reduced, thus advancing the government's interest in improving the quality of service provided by Internet service providers.

The fourth prong is most troublesome because the legislation must be "no more extensive than necessary" to protect the government's interests.[99] One can reasonably foresee an argument from spammers that the proposed legislation is too restrictive because it essentially prohibits them from advertising on-line once recipients click a button and elect not to receive future e-mails. Since the government cannot rely merely on the recitation of harms it seeks to prevent,[100] it will have to present evidence that the harms are real.[101]

---

[94] *Cf.* Greater New Orleans Broadcasting Ass'n, Inc. v. United States, 527 U.S. 173, 174 (1999) (holding that prohibition on broadcasting lottery information could not be applied to advertisements of lawful private casinos where such gambling was legal).

[95] *Central Hudson Gas*, 447 U.S. at 566.

[96] *Id.*

[97] Posadas de Puerto Rico Assocs. v. Tourism Co. of Puerto Rico, 478 U.S. 328, 341 (1986).

[98] Edenfield v. Fane, 507 U.S. 761, 770-71 (1983).

[99] The *Central Hudson* standard is considered intermediate scrutiny. Florida Bar v. Went For It, Inc., 515 U.S. 618, 623 (1995). *See also Edenfield*, 507 U.S. at 768 ("Unlike rational basis review, the *Central Hudson* standard does not permit [the Court] to supplant the precise interests put forward by the [government] with other suppositions.").

[100] *See* Rubin v. Coors Brewing Co., 514 U.S. 476, 489-91 (1995) (invalidating a law that

Moreover, the junk advertisers would point out that if the legislature were truly motivated by individual privacy concerns, one would expect it to regulate other forms of unsolicited advertising such as regular mail, facsimile and telephone advertising; means of advertising media the government has not attempted to regulate.

As a result, any proposed legislation regulating unsolicited e-mail will almost certainly be challenged on First Amendment grounds. Courts will then evaluate the law under the *Central Hudson* test. The key to any *Central Hudson* evaluation will be whether the government's interests can be protected with less restrictive means.

IX. CONCLUSION

Based on the limited case law and proposed federal legislation discussed, it appears that junk e-mail, or spam, will not be afforded significant First Amendment protection. Indeed, courts appear sympathetic to ISPs' fears that people will drop e-mail accounts if the proliferation of mass spamming continues.[102] Nevertheless, it is not clear whether appellate courts will follow the reasoning of the district courts, given the fact that there is a whole line of case law in the commercial speech area that affords limited protection to truthful commercial advertisements. In addition, it is still unclear how much First Amendment protection the Internet will receive.[103]

As Congress and state legislatures continue to propose legislation designed to curb spamming, it will not be long before legislation dealing directly with junk e-mail is passed. Once the law is passed and enforced, one can expect the junk e-mailers to bring a lawsuit challenging the legislation on constitutional grounds.[104] Do not

---

prohibited the advertisement of alcohol content on beer labels where there were alternative and less intrusive means of protecting the government's interest in preventing 'strength wars' between beer manufacturers).

[101] This evidence will likely consist of studies and surveys regarding the actual impact of such anti-spam legislation on the quality of Internet service and the protection of individual privacy, the main interests that the proposed legislation seeks to protect.

[102] Courts likely will be even more sympathetic when the on-line service providers fight to prevent spammers from sending pornographic-related junk e-mail. Am. Online v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998).

[103] *See* Reno v. ACLU, 521 U.S. 844 (1997).

[104] For a review of current legislation and proposals visit these sites: JUNK E-MAIL CALL TO ACTION *at* http://www.tigerden.com/junkmail (last visited April 22, 2001);
Center for Information Technology and Privacy Law, John Marshall Law School, *Unsolicited E-mail Statutes at* http//www.jmls.edu/cyber/statutes/email/index.html (last visited April 22, 2001) and David E. Sorkin, *Spam Laws at* http://www.spamlaws.com (last visited April 22, 2001).

expect these recent defeats in the courts to deter spammers[105] because as we all know, one man's "junk" is another man's "gold."

[105] Recently, one 'spammer' successfully challenged Washington state's anti-spam law as a violation of the interstate commerce clause of the United States Constitution. In striking down the law, the state trial judge found that it was "unduly restrictive and burdensome." The decision is being appealed by the Washington Attorney General's office. *See* Peter Lewis, *Anti-Spam E-Mail Suit Tossed Out*, SEATTLE TIMES, Mar. 14, 2000, at A1.